What's in a name? De juridische status van een recht op anonimiteit

Prins, J.E.J.

Published in:
Privacy en informatie

Publication date:
2000

Document Version
Early version, also known as pre-print

Prins, J.E.J. (2000). What's in a name? De juridische status van een recht op anonimiteit.. Verschenen in: *Privacy en informatie*, *3*(4), 153-157

What's in a name? de juridische status van een recht op anonimiteit[1]

Prof. mr. J.E.J. Prins

Samenvatting
Anonimiteit op het Internet mag zich in een grote belangstelling verheugen. Met name in de discussie over adequate privacybescherming voor consumenten op het Internet wordt gewezen op het belang en de mogelijkheden van het op anonieme basis communiceren en verrichten van transacties. Er wordt inmiddels gesproken over *een recht op anonimiteit.* Stel consumenten krijgen een dergelijk recht en gaan grootschalig anonimiseringstechnieken inzetten om daarmee niet alleen te chatten, te surfen en te zoeken, maar ook om aankopen op het Internet te verrichten: wat zijn daarvan de privaatrechtelijke consequenties? In welke mate laat het Burgerlijk Wetboek toe dat consumenten op anonieme wijze transacties op het Internet verrichten? Kortom, in hoeverre zijn anonieme transacties een realiteit?

Trefwoorden: anonimiteit, pseudoniem, (grond)recht op anonimiteit, privaatrechtelijke status

1. Recht op regie

"Het kabinet zal nagaan op welke wijze invulling kan worden gegeven aan een 'recht op regie over de eigen persoonsgegevens'. Minister Van Boxtel presenteerde het voorstel voor deze verkenning in zijn op 19 mei 2000 verschenen nota *Contract met de toekomst. Een Visie op de elektronische relatie overheid-burger.*[2] Het voornemen van de Minister is deels opvallend, deels ook weer niet. Opvallend, omdat Van Boxtel kennelijk een visie op privacy hanteert die in Nederland nooit echt ingang heeft gevonden. Niet zo opvallend daarentegen, omdat de verkenning past in een tendens waarin anonimiteit bij het handelen op de elektronische snelweg als een belangrijke waarde of zelfs een 'recht' wordt aangemerkt.

Zoals gezegd, kennelijk uitgangspunt voor Minister Van Boxtel is dat privacy een vorm van individuele zeggenschap is: privacy is autonomie. In deze opvatting is het aan de burgers om het persoonsgegevensgebruik door de overheid zelf te beheersen: zij hebben de regie. Deze visie is op opvallend omdat Nederland, anders dan Duitsland, waar

---

[1] Dit artikel bevat resultaten van een onderzoek uitgevoerd binnen een meeromvattend onderzoeksprogramma naar duurzame juridische en organisatorische transformatieprocessen ten gevolge van nieuwe informatie- en communicatietechnologie. Dit onderzoeksprogramma is een initiatief van het Expertise Centrum 'Globalization and sustainable development' aan de Katholieke Universiteit Brabant (KUB) in Tilburg. Het onderzoek geschiedt in samenwerking tussen het Schoordijkinstituut van de Katholieke Universiteit Brabant en de directie algemene justitiële strategie van het Ministerie van Justitie. De auteur dankt mr. dr. J.H.A.M. Grijpink voor zijn inbreng in het onderzoek.

[2] Nota *Contract met de toekomst. Een Visie op de elektronische relatie overheid-burger*, 19 mei 2000, p. 28.

het *Bundesverfassungsgericht* een Grondwettelijk recht op informationele zelfbeschikking heeft erkend, dit uitgangspunt van zeggenschap van het individu over zijn gegevens nooit heeft willen aanvaarden. Ook de Commissie Grondrechten in het digitale tijdperk, die nog geen week na het verschijnen van de Nota van Van Boxtel haar rapport publiceerde, volgt deze lijn en wijst een recht op informationele zelfbeschikking af. De Commissie merkt daarbij zelfs op dat de introductie van een recht op informationele zelfbeschikking weinig toegevoegde waarde heeft.[3]

Van Boxtel is eerder dit jaar voor een oriënterend bezoek naar de Verenigde Staten geweest. Aldaar heeft hij zich laten voorlichten over de invloed van ICT op de relatie overheid-burger. Wie weet heeft Van Boxtel zijn visie op privacy ook aldaar laten vormen. Immers, juist in de Verenigde Staten is de voornoemde visie op privacy – privacy als een vorm van individuele zeggenschap – zeker niet onbekend. Zowel in de doctrine als in de rechtspraak is privacy al langere tijd geïnterpreteerd als een bepaalde vorm van het zelfbeschikkingsrecht: burgers hebben het recht om zelf te beslissen in een aantal privé aangelegenheden.[4] Overigens is ook in de jurisprudentie onder het Europese Verdrag voor de Rechten van Mens een dergelijke visie waar te nemen.[5]

Het spreekt voor zich dat het probleem in de visie op privacy als autonomie zich concentreert rondom de discussie hoe ver precies de eigen regie van een individu gaat bij de keuzes ten aanzien van het beschermen van de privé-sfeer enerzijds, en het algemeen belang anderzijds. De overheid heeft immers ook de plicht het algemeen belang te dienen en heeft daartoe noodzakelijkerwijs persoonsgegevens nodig – ook indien de burger de betreffende gegevens niet wenst over te dragen. Dit normatieve conflict is duidelijk aanwezig in de Amerikaanse discussie over privacybelangen, zeer recentelijk bijvoorbeeld in het boek van de Amerikaanse communitarist Etzioni.[6]

2. Recht op anonimiteit

Een recht op regie over de persoonsgegevens komt in de buurt van een recht op anonimiteit. Immers, uitgangspunt bij een recht op regie is anonimiteit en niet kenbaarheid. Het voorstel voor de introductie van een recht op anonimiteit kan zich over

[3] Rapport Commissie Grondrechten in het digitale tijdperk, Den Haag, mei 2000, p. 126.

[4] Zie met name de uitspraken in de jaren zestig en zeventig in: *Griswold v. Conneticut*, 381 U.S. 479 (1965); *Loving v. Virginia*, 388 U.S. 1 (1967); *Eisenstadt v. Baird,* 405 U.S. 438 (1972); *Roe v. Wade*, 410 U.S. 367 (1973).

[5] Zie: ECRM 18 mei 1976, 6825/74, D&R 5, p. 86 (X v. Iceland); ECRM 12 juli 1977, 6959/75, D&R 1978 (Brüggeman en Scheuten); EHRM 23 september 1981, 7525/76, A45 (Dudgeon). Zie meer in detail: P. Blok, A. Vedder, 'Privacy in ontwikkeling', in: Privacyregulering in theorie en praktijk (red. J.M.A. Berkvens, J.E.J. Prins), Deventer 2000 (te verschijnen).

[6] A. Etzioni, The limits of privacy, New York 1999.

een toenemende belangstelling verheugen.[7] Inmiddels hebben zich diverse voorstanders van de introductie van een dergelijk recht gemeld.[8] Het was opnieuw Minister Van Boxtel die tijdens de parlementaire behandeling van de Wbp aangaf, te bezien of het mogelijk is om burgers ten behoeve van de digitale communicatie met de overheid "anoniem of pseudo-certificaten beschikbaar te stellen waarbij gegevens van de persoon losgekoppeld worden van de persoon zelf."[9] De Raad voor het Openbaar Bestuur kwam in januari 2000 met het rapport "ICT en het recht om anoniem te zijn".[10] Alhoewel de titel veel suggereert, gaat de Raad in het rapport zelf helaas nauwelijks in op de problematiek van anonimiteit.

Op een internationaal niveau heeft men eveneens oog voor het belang van anonimisering.[11] Zo stelt de Raad van Europa dat anonimiteit essentieel is voor privacybescherming op de elektronische snelweg.[12] Hiernaast kan gewezen worden op de Europese richtlijn inzake privacy en telecommunicatie, art. 2 van de Duitse Multimediawet (IuKDG)[13] en Recommendation 3/97 van de artikel-29 werkgroep, getiteld "Anonymity on the Internet".[14] In deze Aanbeveling worden diverse voorbeelden van anonimiserende diensten genoemd: anonimiserende servers en remailers. Wanneer een afzender van een e-mailbericht of een nieuwsgroepbericht van deze laatste gebruik maakt wordt het bericht door de aanbieder van de remailer-dienst 'ontdaan' van de identificerende gegevens alvorens het wordt doorgezonden aan de beoogd ontvanger van het bericht. De werkgroep wijst ook op de mogelijkheden die chipkaarten met een

---

[7] Zie bijvoorbeeld de diverse bijdragen in de speciale editie over anonimiteit van het tijdschrift *The Information Society* (http://web.mit.edu/gtmarx/www/anon.html

[8] Zie: K. Spaink, Parool 28 juni 1999; L. Asscher, Niemand als consument. Naar een evenwichtig grondrecht op anonimiteit', in: De *e*-Consument. Consumentenbescherming in de Nieuwe Economie, Elsevier 2000 (te verschijnen).

[9] TK '99-'00, 25 892, nr. (vergadering 17 november 1999).

[10] Raad voor het Openbaar Bestuur, 'ICT en het recht om anoniem te zijn', Den Haag, januari 2000.

[11] Zie bijvoorbeeld art. 8, lid 3, van de Richtlijn elektronische handtekening. Pb EG 2000 L 13/12.

[12] Guidelines Raad van Europa, 1997: "Guidelines for the protection of individuals with regard to the collection and processing of personal data on the information highways, which may be incorporated in or annexed to codes of conduct", Project Group on Data Protection, Council of Europe, 17 October 1997, CJ-PD (97) rev. , II, nr. 3.

[13] Officieel: Informations- und Kommunikationsdienste-Gesetz, BT-Drucksache 13/7934, in werking getreden op 1 augustus 1997 (te vinden op: www.iid.de/rahmen/iukdgbt.html.

[14] XV D/5022/97 final, 1997. Te raadplegen op de site van DG XV.

bepaald Internet-tegoed bieden, zodat aldus anoniem voor bepaalde diensten of producten kan worden betaald.

Er zijn natuurlijk ook de tegenstanders van een recht op anonimiteit. Eind 1999 stonden de media vol van het bericht dat het VVD-kamerlid Cherribi anoniem surf- en communicatiegedrag op het Internet strafbaar wilde stellen. Aanleiding voor de actie van het kamerlid vormde de introductie in Nederland, door Internet Provider XS4All, van de Freedom-software. Met deze software kan een gebruiker zelf een anonieme elektronische identiteit ('nym') aanmaken en bestaan er geen mogelijkheden tot terugkoppeling tussen de werkelijke naam van de gebruiker en de gekozen elektronische identiteit. Ook de Provider als tussenpersoon kan de link tussen de beide identiteiten niet leggen.[15]

Wat betreft de tegenstanders van een recht op anonimiteit moet natuurlijk ook worden gewezen op de ontwikkelingen in Frankrijk. Daar lanceerde de Senaat begin 2000 een wetsvoorstel om anoniem publiceren en anonieme web-hosting op het Internet te verbieden.[16]

3. Belangen bij anonimiteit

In Nederland kwam de discussie rondom het belang van anonimiteit in een informatiemaatschappij voor het eerst duidelijk naar voren bij de introductie van de prepaid kaart voor mobiele telefonie. De regering leek eind 1997 in eerste instantie niet zo blij met deze mogelijkheid. De toenmalige Minister van Binnenlandse Zaken stelde dat de regering plannen had om te komen tot een verbod op anoniem gebruik van prepaid kaarten voor mobiele telefoons. Nadat de Registratiekamer de regering in een kritisch advies verzocht het voornemen te heroverwegen, was het van de baan. Volgens de Registratiekamer zou het loslaten van het uitgangspunt van anonieme communicatie in dit verband resulteren in een onrechtmatige inbreuk op het recht op vertrouwelijke communicatie zoals neergelegd in artikel 8 EVRM.[17] Begin 1998 stelde de regering in de Nota 'Wetgeving voor de elektronische snelweg' zelf ook dat anonimiteit bij het handelen op de elektronische snelweg het uitgangspunt moet zijn. [18],

Van oudsher is de ratio van anonimiteit gelegen in een diversiteit van belangen. Los van de specifieke omstandigheden van het Internet kan gewezen worden op het recht om zelf het moment te bepalen waarop informatie openbaar wordt, het afschermen van informatiebronnen, het onderhouden van contacten en relaties met uitsluiting van derden en het recht om zonder inmenging van anderen te communiceren en overleg te voeren. Deze belangen sluiten nauw aan bij het recht van een ieder op eerbiediging van zijn privéleven en zijn communicatie, zoals erkend in artikel 8 EVRM.

---

[15] www.zeroknowledge.com/media/freedom-fs.asp

[16] Zie: http://www.senat.fr/seances/s200001/s20000119/sc20000119005.html

[17] Registratiekamer, 12 december 1997.

[18] TK 1997-1998, 25880, nrs. 1-2, p. 129.

Mensen die in bepaalde situaties anoniem wensen te blijven in hun handelen, hebben soms echter wel de behoefte 'herkenbaar' te zijn. De bekendste voorbeelden zijn te vinden in de literaire en muziekwereld. Auteurs wensen weliswaar hun ware naam niet te onthullen, maar willen zich wel naar een grotere groep individualiseren (en aldus met hun werk herkenbaar zijn). Hiertoe hanteren ze een pseudoniem. Er zijn overigens ook andere redenen waarom bepaalde auteurs zich niet onder hun ware naam bekend maken : zo kan de verzonnen naam beter aanslaan bij het publiek of wordt het pseudoniem gekozen uit mode-overwegingen.

Ook in een elektronische omgeving wensen mensen soms anoniem, maar toch herkenbaar te zijn. Een voorbeeld is het 'chatten'. In dit geval gaat het ook om de algemene bekendheid onder het pseudoniem (veelal 'nym' genoemd). Bij andere toepassingen van een digitaal pseudoniem gaat het echter niet om algemene kenbaarheid, maar om de kenbaarheid naar individuele (rechts)personen in relatie tot individuele transacties. Met de inzet van computertechnologie is het ook mogelijk om onuitspreekbare woorden of bepaalde getalcombinaties, die voorheen niet als pseudoniem maar als anonimiteitsteken werden aangemerkt, te laten fungeren als pseudoniem (PIN-code). In dit geval is het oogmerk een betrouwbare elektronische verificatie. Het is niet langer de mens die hier het pseudoniem individualiseert, maar een machine. Daarbij komt dat bij de PIN-situaties het veelal niet de handelend persoon zelf is die kiest voor het gebruik van een pseudoniem, maar het de aanbieder van een bepaalde dienst is die dit als voorwaarde voor het gebruik daarvan stelt. Naast verificatie, is een eventueel tweede oogmerk de handeling aan een bepaald persoon te kunnen relateren gelegen in de mogelijkheid om deze persoon op zijn handelen te kunnen aanspreken (bijvoorbeeld bij fraude). Dit betekent dat het pseudoniem te herleiden moet zijn tot de daadwerkelijke identiteit en dat individualiseerbaarheid dan te maken heeft met traceerbaarheid. Bij een dergelijk elektronisch pseudoniem zal de individuele *persoonlijkheid* van de persoon die de handeling verricht veelal niet relevant zijn. Wel zal de persoon als zodanig relevant zijn in verband met kwesties van risicotoedeling en verhaalbaarheid. Dit betekent dat een elektronisch pseudoniem in veel gevallen in feite overdraagbaar is. Contractueel kan – zoals met de PIN gebeurt - natuurlijk anders afgesproken worden, bijvoorbeeld om redenen van aansprakelijkheid.[19]

De belangrijkste reden voor consumenten om op het Internet hun identiteit te verhullen is momenteel gelegen in de wens niet te worden blootgesteld aan de informatiedrang van derden. Kort gezegd is het belang gelegen in privacyoverwegingen. Een pseudoniem is in deze gevallen ook niet nodig. Toepassingen als Freedom zijn primair ontwikkeld om gebruikers van het Internet de mogelijkheid te bieden tot het

[19]Overigens kan de toegepaste techniek een overdracht feitelijk in de weg staan. Vgl. bijvoorbeeld biometrie.

anoniem verzenden van e-mails, het anoniem zoeken van informatie op websites, anoniem chatten, anonieme deelname aan spelletjes, etc.

4. De relativiteit van anonimiteit

Vele van de momenteel in omloop zijnde technieken om anonimiteit te bewerkstelligen werken op basis van het principe dat de in beginsel anonieme berichten onder omstandigheden toch tot de betrokken persoon kunnen worden herleid. In feite is er dus geen sprake van echte anonimiteit. Voorbeelden hiervan zijn de chipknip en andere virtuele betaalmiddelen. Veelal is slechts sprake van pseudo-anonimiteit. Met de Freedom-software is de stap gezet naar daadwerkelijk anonimiserende technieken op het Internet. Ook biometrie biedt belangrijke mogelijkheden voor volledig anoniem handelen. We kunnen aldus stellen dat anonimiteit meerdere dimensies heeft. Dit is zeker het geval als we tevens de situaties meenemen waarin personen weliswaar anoniem handelen, maar toch herkenbaar zijn (een pseudoniem gebruiken). In feite kunnen we dan de onderstaande vier gradaties van anonimiteit onderscheiden.

handelen onder een pseudoniem

Bij een pseudoniem wordt, zoals hiervoor opgemerkt, gebruik gemaakt van een onderscheidingsteken waarmee een bepaalde transactie of handeling tot een bepaalde persoon is terug te herleiden. Wie precies deze persoon is behoeft niet kenbaar te zijn. Het gaat om kenbaarheid of verifieerbaarheid, niet om identificeerbaarheid. Pseudonimiteit kan worden bewerkstelligd middels een ‘nym’, maar ook een reeks van getallen, een digitale afdruk van een vinger, of middels gezichtsherkenning.[20] De belangrijkste reden om onder een pseudoniem handelingen en transacties te verrichten is dat de persoon die het pseudoniem hanteert zich daarmee (her)kenbaar maakt voor de buitenwereld. De betreffende personen wensen weliswaar hun ware naam niet te onthullen, maar willen zich wel naar een grotere groep individualiseren (en aldus met hun handelen, chatten, etc. herkenbaar zijn). Zo kan iemand met behulp van een pseudoniem in discussiegroepen participeren en onder zijn/haar ‘nym’ herkend worden. Ook kan iemand zich middels een PIN-code behorende bij een chipkaart laten verifieren.

Handelen onder een pseudoniem kan in twee vormen: semi-pseudoniem en volstrekt pseudoniem.

- Semi-pseudoniem: in dit geval blijven de handelingen voor bepaalde instanties of tussenpersonen identificeerbaar wanneer de omstandigheden daartoe aanleiding geven. Zo blijft de consument bij het betalen met behulp van een chipkaart anoniem voor de winkelier, maar kunnen de banken deze consument traceren wanneer sprake is van een eventuele fraude met betrekking tot de chipkaart. Kortom, terwijl de consument in diens relatie met de winkelier onder een volstrekt pseudoniem (een

[20]Zie: www.id-arts.com.

PIN) handelt, doet hij dat niet in de relatie met de bank. Aldaar is sprake van een semi-pseudoniem. Ook bij het gebruik van een 'nym' verkregen via een anonymizer voor participatie in discussiegroepen, waarbij de identificerende gegevens echter wel bekend zijn bij deze anonymizer, is sprake van handelen onder een semi-pseudoniem.

- Volstrekt pseudoniem. Bij het handelen onder een volstrekt pseudoniem is van traceerbaarheid geen sprake meer omdat de identiteit van de handelend persoon op geen enkele wijze kan worden vastgesteld. Een dergelijke situatie kan bereikt worden door een keten van anonymizers in te schakelen en bovendien te werken met versleutelde berichten. Aldus zal het feitelijk welhaast onmogelijk zijn de identiteit van de afzender van het bericht te achterhalen. Zo publiceerde het Canadese softwarebedrijf *Zero-Knowledge* begin 2000 een plan voor webbetalingen waarbij het onmogelijk is de identiteit van de betalende persoon te achterhalen. Gebruikers behoeven in dit geval bij betaling met digitaal geld op het Internet niet langer diverse persoonsgegevens aan te leveren, maar krijgen een certificaat waarop bijvoorbeeld hun leeftijd staat, vergezeld van een pseudoniem.[21]

anoniem handelen

In tegenstelling tot het handelen onder een pseudoniem, wordt bij anonieme handelingen geen gebruik gemaakt van een onderscheidingsteken waarmee een bepaalde transactie of handeling tot een bepaalde persoon is terug te herleiden. Het oogmerk zich naar een grotere groep te willen individualiseren speelt hier geen rol bij de wens om de eigen identiteit in een elektronische omgeving te verhullen. Ook hier weer twee vormen aannemen:

- Semi anoniem: bij dergelijke handelingen is voor de buitenwereld sprake van een anonieme handeling. Toch blijft de afzender kenbaar voor bepaalde personen omdat de identificerende gegevens gedurende een periode beschikbaar blijven. Zo zijn de handelingen in bepaalde situaties voor bepaalde instanties of tussenpersonen nog steeds verifieerbaar. Als voorbeeld van semi-anonieme handelingen kunnen de remaildiensten op het Internet genoemd worden. Met name wanneer slechts één anonimiseringsdienst (remailer) wordt ingeschakeld moet de handeling als semi-anoniem worden gekwalificeerd. De remailer houdt de identificerende gegevens veelal gedurende een bepaalde tijd voorhanden en kan ze in bepaalde situaties – bijvoorbeeld op last van justitie - beschikbaar stellen. Wanneer het hiervoor beschreven scenario van een keten van remailers wordt toegepast, zal men – afhankelijk van de hoeveelheid gebruikte remailers - opschuiven naar een volledig anonieme handeling. Immers, met een toenemend aantal schakels in de keten zal het feitelijk steeds moeilijker worden de afzender van het bericht te achterhalen.

[21] http://www.webwereld.nl/nieuws/printout.phtml?id=3820

- Volstrekt anoniem: bij volstrekte anonimiteit is van traceerbaarheid geen sprake meer omdat de identiteit van de handelend persoon op geen enkele wijze kan worden vastgesteld. Te denken valt bijvoorbeeld aan een gebruiker die – bijvoorbeeld in een Internetcafé of een openbare bibliotheek - een bepaalde on-line tijd heeft gekocht en daarbij van de bibliotheek een anoniem e-mail adres heeft gekregen. Toepassingen waarbij anonimiteit een eigenschap van de techniek zelf is zijn er op het Internet nog zeer spaarzaam. Zoals hiervoor reeds genoemd, lanceerde Internet Provider XS4ALL eind 1999 Freedom, waarmee gebruikers anoniem kunnen surfen, e-mailen en chatten. Van volledig anonieme transacties is momenteel nog geen sprake. Een andere ontwikkeling betreft het gebruik van biometrische gegevens of genetische informatie (bijvoorbeeld uit menselijke cellen) ten behoeve van het on-line identificeren van personen. Bij deze laatste technologie wordt de informatie uit menselijke cellen gedigitaliseerd en verkrijgt de gebruiker daarmee een eigen volstrekt unieke identificatiecode. Wanneer een dergelijke 'genetische vingerafdruk' niet wordt gekoppeld aan andere gegevens van de betreffende persoon is de identiteit van deze niet te achterhalen en is sprake van volledig anonieme handelingen.[22]

Kijken we naar de praktijk op het Internet, dan stellen we vast dat momenteel in bijna alle gevallen dat wordt gesproken over anonimiteit sprake van semi-anonimiteit dan wel semi-pseudonimiteit. De handelingen zijn voor bepaalde instanties of tussenpersonen immers nog steeds verifieerbaar wanneer de omstandigheden daartoe aanleiding geven. Bij de anonimiseringsdiensten op het Internet behoudt de remailer zich in de algemene voorwaarden veelal het recht voor de identiteitsgegevens in bepaalde gevallen aan de daartoe bevoegde instanties af te geven.[23] Desalniettemin komen er toepassingen die volstrekte anonimiteit dan wel pseudonimiteit bieden. De vraag die dan naar voren treedt is in hoeverre ons recht ruimte laat voor dergelijke handelingen. In hoeverre kunnen we op het Internet aankopen doen en aldus rechtshandelingen verrichten zonder dat de identiteit bekend is?[24]

5. Anonimiteit en het verbintenissenrecht

[22] 'Genetische vingerafdruk identificeert online', Computable, 22 februari 2000. Over biometrie, zie: Robert van Kralingen, Corien Prins en Jan Grijpink, *Het lichaam als sleutel*, *juridische beschouwingen over biometrie*, IT&R-reeks nr 8, Samson, Alphen a/d Rijn, november 1997

.

[23] Zie bijvoorbeeld artikel 8 van de voorwaarden van anonymizer.com (www.anonymizer.com/3.0/services/agreement.shtml).

.

[24] Over de strafrechtelijke aspecten wordt door de auteur een andere publikatie voorbereid. Zie voor de problematiek in de fysieke wereld: G.J.M. Corstens, Anonymi in het strafproces, DD 17(1987), pp. 339-346; H.K. Elzinga, In beroep, Gouda Quint 1999, pp. 53-61.

Anonieme transacties vormen geen nieuw verschijnsel in het privaatrecht. In de praktijk van alle dag vinden reeds lange tijd diverse rechtshandelingen plaats waarbij een der partijen anoniem blijft omdat ter plaatse en contant voor een product of dienst wordt betaald. Wanneer een student contant een gulden in een koffie-automaat werpt voor een beker espresso, ontstaat een rechtsverbintenis, al zal hij of zij daar niet als zodanig bij stil staan. Het feit dat partijen tot overeenstemming komen zonder dat zij daarbij elkaars identiteit kennen, ontzegt de verbintenis geen rechtskracht: ook deze overeenstemming resulteert in principe in een rechtens verbindende overeenkomst.[25]
Problemen ontstaan eerst wanneer het resultaat van de verbintenis uitblijft dan wel om andere redenen de verbintenis niet wordt nagekomen: de eerdergenoemde student krijgt thee in plaats van espresso uit de automaat.

Bij het instellen van een vordering tot schadevergoeding zal de schuldeiser met lege handen blijven staan wanneer de identiteit van de wederpartij hem niet bekend is. Problemen treden eveneens naar voren in de gevallen van niet-tijdige nakoming waar een ingebrekestelling is vereist. Art. 6:82, eerste lid, B.W. stelt dat het verzuim van een schuldenaar intreedt, wanneer de schuldenaar in gebreke wordt gesteld bij een schriftelijke mededeling. Ook voor andere in relatie tot niet-nakoming voorhanden instrumenten zoals het recht van reclame (art. 7:39 B.W.) en de mogelijkheid tot het vernietigen van een rechtshandeling is het wenselijk dat de identiteit van de niet-nakomende partij bekend is.

Een blik op de rechtspraak inzake de obligatoire (verbintenisscheppende) overeenkomst leert dat de identiteit van een der partijen ook een rol kan spelen bij de kwalificatie van de overeenkomst. Art. 6:217 B.W. stelt dat een overeenkomst tot stand komt door een aanbod en de aanvaarding daarvan. Van belang hierbij is dat het aanbod duidelijkheid verschaft over de belangrijkste verplichtingen die uit de overeenkomst zullen voortvloeien. Bij onvoldoende duidelijkheid hierover is slechts sprake van een *uitnodiging* tot het doen van een aanbod. De vereiste duidelijkheid kan mede duidelijkheid omtrent de identiteit van een der partijen inhouden.[26].

Een nadere aanduiding van de wederpartij is eveneens van belang gegeven de hoedanigheid van contractspartijen (consument, detaillist, werknemer, etc.). Kenbaarheid hiervan blijkt in diverse situaties van belang te zijn voor de toepasselijkheid van bepaalde bepalingen uit het Burgerlijk Wetboek. Gewezen kan onder meer worden op de grenzen die het B.W. stelt aan de contractsvrijheid van partijen wanneer een der partijen consument is. Een ander voorbeeld betreft de consumentenkoop. Hier is het criterium dat de verkoper handelt in de uitoefening van een beroep of bedrijf en de koper een natuurlijk persoon is die niet handelt in de uitoefening van een beroep of bedrijf (art. 7:5, eerste lid,

[25] In het zakenrecht treffen we echter een andere situatie aan omdat voor een groot aantal zakenrechtelijke transacties inschrijving in een register is vereist.
[26] HR 10 april 1981, NJ 1981, 532; Hofland/Hennis.

B.W.).[27] De bepalingen inzake consumentenkoop gaan er van uit dat de hoedanigheid van de contractspartijen bekend is. Ze vereisen dus geen kennis van de identiteit van de consument, maar het bestaansrecht van dergelijke bepalingen komt op de tocht te staan wanneer het niet duidelijk is met welk type contractspartij de aanbieder van doen heeft. Indien een aanbieder op het Internet de identiteit van de consument niet kent, zal hij in de meerderheid van de gevallen immers ook niet weten met een consument van doen te hebben.

6. Risico-toedeling van elektronische anonimiteit

Het bovenstaande leert dat in het B.W. de identiteit van een der partijen als zodanig niet altijd ter zake doet. Kortweg: in het verbintenissenrecht is de identiteit geen wettelijk vereiste. Desalniettemin speelt de identiteit van contractspartijen wel degelijk een rol bij de nadere invulling en uitwerking van de relevante vereisten uit het B.W. In veel gevallen is het belang van kenbaarheid gelegen in de wens een aanspreekbaar subject te hebben.

Wat nu indien een rechtshandeling door een consument op volstrekt anonieme basis is verricht, maar deze consument zijn verplichtingen niet nakomt? In de regel bestaat in deze gevallen aanspraak op diverse acties (nakoming, schadevergoeding). Doch, gegeven de omstandigheid dat de identiteit van de consument niet bekend is aan de aanbieder zal een (schadevergoedings)actie op grond van een tekortkoming weinig soulaas bieden. De schadevergoedingsvordering van de schuldeiser is op feitelijke gronden uitgesloten omdat het voor de schuldeiser onmogelijk is de debiteur aan te spreken.

Gegeven de mate waarin met de huidige technologische toepassingen volstrekte anonimiteit bewerkstelligd kan worden is er vooralsnog onvoldoende aanleiding tot een andere conclusie te komen dan dat wanneer de aanbieder bewust het risico neemt een overeenkomst aan te gaan met een volstrekt anonieme wederpartij, hij het risico van de nadelige gevolgen van de tekortkoming draagt. Evenals in de fysieke wereld verkrijgt hij noch de prestatie waartoe de consument gehouden was, noch schadevergoeding. Wat betreft de gevolgen van de onmogelijkheid voor de aanbieder om wetenschap te hebben betreffende de hoedanigheid waarin diens wederpartij handelt (bijvoorbeeld als consument) moeten deze gevolgen in principe aan deze wederpartij worden toegerekend. Indien een consument gebruik wil maken van de grenzen die het recht stelt aan de contractsvrijheid van de aanbieder (bijvoorbeeld in relatie tot een (vermoedelijk) onredelijk bezwarend beding) en de vernietigbaarheid van een bepaald beding wil inroepen, zal deze consument zich als zodanig kenbaar dienen te maken. Zolang de betreffende persoon zijn identiteit niet kenbaar maakt, zou mogen worden aangenomen dat hij ook geen beroep kan doen op de speciale beschermingsmaatregelen voor consumenten.

[27] Een ander voorbeeld betreft de specifieke deskundigheid van de wederpartij, welke een rol bij de beoordeling van de aansprakelijk van partijen en daaruit voortvloeiende zorgvuldigheidsverplichtingen.

De uitgangspunten inzake de risicotoedeling bij volstrekt anonieme elektronische transacties verschillen niet van die welke momenteel in ons recht aanvaard zijn voor anonieme transacties in een fysieke wereld. Er is momenteel ook geen directe aanleiding om middels wettelijk ingrijpen tot een andere risicoverdeling over te gaan. Toch kan er een moment komen dat hiertoe wel aanleiding bestaat. Immers, de elektronische dimensie zou de problematiek van volstrekte anonimiteit kunnen vergroten met als gevolg dat de risico's in toenemende mate bij de zwakkere partij – de consument die anoniem wenst te handelen – worden gelegd. Zo kan de combinatie van anonimiteit en transacties op afstand, met aldus juridische implicaties onder een voor consumenten vreemd recht, een nieuwe dimensie toevoegen. Een ander aspect is de huidige praktijk van volledige betaling vooraf door de consument. Wat is de (bewijs)positie van een consument die op anonieme wijze een bepaald produkt heeft aangeschaft, daarvoor reeds het volledige bedrag heeft betaald, maar tot de conclusie komt dat het produkt toch niet aan de vereisten voldoet? Deze en andere risico's zouden consumenten ervan kunnen weerhouden anonieme transacties op het Internet te verrichten. Het recht op anonimiteit is dan in feite niet meer dan een dode letter.

7. Anonimiteit off-line moet ook on-line

Als we vaststellen dat het ontbreken van een aanspreekbaar en in bepaalde situatie in zijn hoedanigheid kenbaar subject onder het verbintennissenrecht bepaalde risico's met zich meebrengt, ligt de vraag voor of dit aanleiding is voor het stellen van aanvullende regels dan wel een aanpassing van het huidige wettelijk kader. De voorkeur lijkt in eerste instantie uit te gaan naar zelfregulering door de markt. Gedurende de periode dat de technische ontwikkelingen met betrekking tot (pseudo-)anonieme handelingen nog niet zijn uitgekristaliseerd, de consequenties daarvan niet volledig zijn te overzien en er behoefte bestaat te experimenteren met bepaalde (technische) randvoorwaarden, kan regulering door de markt zijn waarde bewijzen. Daarbij kan men stellen dat de zich ontwikkelende praktijk ook een aanzet kan bieden voor het ontstaan van nieuwe rechtsnormen ten aanzien van (pseudo-)anoniem handelen. De belangen van consumenten zouden in deze aanpak vertegenwoordigd moeten worden door consumentenorganisaties.

Indien er uiteindelijk toch voor wordt gekozen wetgeving een rol te geven bij het reguleren van pseudo-anonieme rechtshandelingen omdat de risico's onevenredig over de betrokken partijen verdeeld lijken te worden, zal wat betreft de inhoud van de eventuele nadere regels onderzocht moeten worden welke belangen bij de toepassing van anonimiteit beschermd moeten of zouden moeten worden. Anders gezegd: wat beoogt men met een eventuele aanpassing van het bestaande wettelijk regime? Gedacht kan hier worden aan het veiligstellen van bepaalde belangen zoals het vertrouwen in de anonieme elektronische transacties, consumentenbescherming, de bewijspositie van betrokken partijen, het tegengaan van identiteitsfraude en zeker niet te vergeten: de rechtszekerheid.

Bij een eventuele aanpassing van het wettelijk kader zal – gegeven de gewenste inhoud van de regeling - bezien moeten worden welke invloed een dergelijke regulering heeft op de uitgangspunten van het nationale verbintenissenrecht. Gegeven de grensoverschrijdende dimensie van elektronische communicatie en handelingen zou bij het formuleren van de nadere regels tevens gekeken kunnen worden naar de ontwikkelingen en aanknopingspunten in de buitenlandse rechtstradities. Een blik op het Anglo-Amerikaanse rechtssysteem leert dat daar aangrijpingspunten zijn te vinden voor een objectivering (depersonalisatie) van relaties gecombineerd met een aansprakelijkheidssysteem. Wat de personen die op volstrekt anonieme basis handelen precies met hun handelen beogen en wie deze personen precies zijn doet er in een dergelijk systeem niet toe: de handelingen van personen en hun relatie worden gedepersonaliseerd. De aansprakelijkheidskwestie wordt afgedekt met een systeem van objectieve risicoverdeling en de aansprakelijkheidsrisico's kunnen dan worden ondervangen door een te ontwikkelen verzekeringssysteem.

8. Conclusie

We stellen vast dat anoniem handelen zich op het Internet in een grote belangstelling verheugen. Duidelijk is echter ook dat het geen nieuw fenomeen is en er bovendien meerdere dimensies van anonimiteit bestaan. Privaatrechtelijk staat er personen niets in de weg rechtshandelingen te verrichten zonder dat ze daarbij hun identiteit kenbaar maken. Wel resulteert het ontbreken van kennis inzake de identiteit van partijen in problemen bij de uitvoering van de verbintenis. Er moet immers een aanspreekbaar en in bepaalde situaties ook in zijn hoedanigheid kenbaar subject zijn. Het bovenstaande leert dat er vooralsnog geen reden is specifieke wetgeving te introduceren in verband met de risico's die anoniem handelen met zich meebrengt. Uitgesloten kan echter niet worden dat nadere regelgeving is gewenst in verband met belangen zoals consumentenbescherming.

Rest een laatste afrondende conclusie: wat de uitkomst van de diverse ontwikkelingen inzake anonieme en semi-anonieme handelingen op het Internet ook moge zijn, het uitgangspunt bij de privacybescherming van consumenten op het Internet moet zijn dat waar zij in de off-line wereld volledig anoniem bepaalde handelingen willen en kunnen verrichten, ze dit ook in een on-line omgeving moeten kunnen doen. Dit behoeft niet direct te resulteren in een *recht op anonimiteit*, maar wel in een afdoende (wettelijk) raamwerk voor het realiseren van en vertrouwen in anonimiteit. Hiertoe moeten zowel de technische en organisatorische middelen de noodzakelijke mogelijkheden bewerkstelligen, als ook het recht de gewenste ruimte bieden.